



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,016	05/10/2006	Vesa Torvinen	P18450US1	1254
27045	7590	01/13/2011	EXAMINER	
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR 1-C-11 PLANO, TX 75024				BENOIT, ESTHER
ART UNIT		PAPER NUMBER		
2453				
			NOTIFICATION DATE	DELIVERY MODE
			01/13/2011	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com  
jennifer.hardin@ericsson.com  
melissa.rhea@ericsson.com

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/595,016	TORVINEN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	ESTHER BENOIT	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 17 November 2010.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1,2,6,8,13,14,18,23-25 and 30 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1,2,6,8,13,14,18,23-25 and 30 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date. _____ .	6) <input type="checkbox"/> Other: _____ .

## **DETAILED ACTION**

### ***Response to Amendment***

1. This Action is in response to an Amendment filed on November 17, 2010. Claims 1-2, 6-8, 13-14, 18, 23, and 30 have been amended. Claims 3-5, 7, 9-12, 15-17, 19-22, 26-29, and 31-33 are cancelled. Claims 1-2, 6-8, 13-14, 18, 23-25, and 30 are pending in this application.

### ***Response to Arguments***

2. Applicant's arguments filed 11/17/2010 have been fully considered. Some arguments are moot in view of the newly amended limitations and rejection, but some arguments were not persuasive. The arguments that were not found persuasive are addressed below. The applicants are arguing in substance the following:

#### **Arguments under 35 U.S.C. 103 (a)**

##### ***Arguments to Claim 18:***

- a) Reiche does not disclose "sending directly from said remote server to an authentication node in the UE's home network a second request for access".
- b) Reiche does not disclose "a remote server directly sending a second request for access to the authentication server in the UE's home network wherein said second request instructing said authentication node to then generate a challenge to the UE including the temporary identity of the UE and the identity of the remote server".

c) Reiche does not disclose “UE generating a password based on the challenge, said password being associated with the temporary identity of the UE created by said remote server”.

d) Reiche does not disclose “receiving at said remote server a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server”.

e) Inoue does not disclose “a remote server receiving a first request for access from a UE and then sending a second request directly from the remote server to the authentication server residing within the home network, wherein said second request from the remote server containing the temporary identity for the UE as created by that remote server”.

***Response to arguments of Claim 18:***

As to point a: The argument has been considered but is not persuasive. Reiche discloses a transaction ID is created by a customer server and stored in a database at the customer server. The ID is sent to the user along with a redirect request to the central authentication server, where the central authentication server is in charge of authenticating the user (Col. 4, lines 57-67 and Col. 5, lines 1-6).

As to point b: The argument has been considered but is not persuasive. Reiche discloses the central authentication server initiates access grant control procedure in the form of an authentication challenge to the user (Col. 5 lines 15-22).

As to point c: The argument has been considered but is not persuasive. Reiche discloses control is given to the user to enter a user password and supplied to the authentication server (Col. 5 lines 15-22). The password and user ID is based on the transaction ID provided by the customer server the user is wishing to gain access to. (Col. 4, lines 57-67, Col. 5, lines 1-6, and lines 15-31).

As to point d: The argument has been considered but is not persuasive. In Col. 9, lines 57-67, Reiche discloses a verification process that takes place at the customer server for verifying that a client is authenticated with the customer server.

As to point e: The argument has been considered but is not persuasive. The reference Inoue is used to disclose that the authentication node can also reside in the UE's home network ([0092]-[0098]). A registration request is received at the Home Agent along with password and user ID to check if user is legitimate or not.

As to any claims not specifically discussed, the applicants argued that it was patentable for one of the reasons discussed above. Please see response to above arguments for unspecified discussions.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 6-8, 14, 18, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over of Reiche (6,092,196), in view of Inoue et al. (US 2006/0034238 A1).

**With respect to claims 18,** Reiche discloses:

- receiving a first request for access from said UE by said remote server (Col. 8, lines 47-49, *customer server receives request from client to access a URL on the customer server*);
- creating a temporary identity for the UE by said remote server (Col. 8, lines 64-67, *Authentication Daemon inside of customer server detects client is not authenticated and further creates unique client ID for client*);
- sending directly from said remote server to an authentication node, a second request for access including said temporary identity created by said remote server and an identity of said remote server (Col. 9, lines 6-26, *AD in customer server redirects client's browser to authentication server for authenticating the client. AD passes URL string and transaction ID to authentication server, wherein URL string includes client ID*), and instructing said authentication node to generate a challenge including said temporary identity of the UE and said identity of said remote server (Col. 5, lines 15-22 and Col. 9, lines 20-26, a **401 challenge is sent to user's browser to initiate user to enter authentication credentials**)
- at the UE, generating a second password based on the challenge, said password being associated with the temporary identity of the UE created

by said remote server (Col. 9, lines 15-32, *401 authentication challenge is sent back to client's browser causing authentication server to redirect control to user's browser for password input*);

- storing the second password and the temporary identity of the UE at the UE (Col. 9, lines 30-31, *where client's browser retains authentication information*);
- receiving at said remote server a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server (Col. 9, lines 27-37, *client is able to input authentication data received from authentication server in dialog window to show proof that user ID and password have been obtained*) and allowing said remote server and said UE to challenge and authenticate a subsequent access request directly without sending said second request from said remote server to said authentication node (Col. 6, lines 37-56, *allows the browser to automatically release authentication information to the authentication server*)

Reiche does not explicitly disclose the authentication node can also reside in the UE's home network.

However, Inoue discloses the authentication node can also reside in the UE's home network ([0092]-[0098], *registration request is received at Home Agent along with password and user ID to check if user is legitimate or not*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche with the teachings of Inoue to include an authentication node in the home network, *because* it will allow the user secure access to its home network when roaming on a visited network.

**With respect to claim 1**, the limitations of claim 1 are essentially similar to the limitations as claim 18 with a difference of generating first and second passwords. A first password is generated at the authentication node (Reiche, Col. 9, lines 20-25 and Col. 1, lines 55-59, *a 401 challenge generated by authentication server includes header field which consists of authentication parameters [See RFC 2068]*). Second passwords are generated by user after authentication challenge is returned (Reiche, Col. 5, lines 25-30). Therefore, the claim is rejected for the same reasons as claim 18 above. Please see rejection above.

**With respect to claims 6 and 23**, Reiche discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE and is an HTTP Digest challenge (Col. 9, lines 15-32, *401 authentication challenge is sent back to client's browser causing authentication server to redirect control to user's browser for password input*);

**With respect to claims 8 and 25**, Reiche discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the first password has been generated (Col. 9, lines 37-67).

**With respect to claim 14**, Reiche discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (Col. 9, lines 38-67).

**With respect to claim 24**, Reiche discloses the method, wherein the password is stored at the authentication node (Col. 12, lines 61-63)

5. Claims 2, 13, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over of Reiche (6,092,196), in view of Inoue et al. (US 2006/0034238 A1), and further in view of Niemi et al. (RFC 3310, HTTP Digest Authentication Using AKA).

**With respect to claim 2**, Reiche and Inoue does not explicitly disclose said authentication node uses HTTP Digest Authentication and Key Agreement (AKA) for generating first passwords.

However, Niemi discloses the method, wherein the authentication node uses HTTP Digest Authentication and Key Agreement (AKA) for generating first passwords (pg. 6, paragraph 2, “If the server...”, and pg. 7, paragraph 1, “When a client...”)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche and Inoue with the teachings of Niemi to use HTTP Digest Authentication and Key Agreement, *because it will allow for better password encryption.*

**With respect to claims 13 and 30**, Reiche discloses authenticating the UE at the remote server (Col. 9, lines 22-36)

Reiche and Inoue do not explicitly disclose a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server.

However, Niemi discloses HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server (pg. 6, paragraph 2, "If the server...", and pg. 7, paragraph 1, "When a client...")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Reiche and Inoue with the teachings of Niemi to use HTTP Digest Authentication and Key Agreement, *because* it will allow for better password encryption.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esther Benoit whose telephone number is 571-270-3807. The examiner can normally be reached on Monday through Friday between 7:30 a.m and 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista M. Zele can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.B.  
January 10, 2011

/Krista M. Zele/  
Supervisory Patent Examiner, Art Unit 2453

Application/Control Number: 10/595,016  
Art Unit: 2453

Page 11